Kan de zelflerende machine u beter beschermen?

Algoritmes die zichzelf verbeteren worden vaak genoemd om ziektebeelden te herkennen, of zelfrijdende wagens te sturen. Maar ook in het razendsnel evoluerende securitylandschap brengt machine learning de extra versnelling om cybercriminelen te snel af te zijn. **Pieterjan Van Leemputten**

Het zijn hoogdagen voor securitybedrijven. De hack bij het Amerikaanse Equifax is een uitgelezen kans om te wijzen op het belang van een goede beveiliging. Hier lag het probleem op te laat gepatchte servers, maar ook het ontdekken van hackers op uw netwerk duurt soms maanden. Tegelijk wordt duidelijk dat populaire plaatsen zoals de Play Store van Google probleemloos gevuld kunnen worden met malafide apps en dat ook iOS niet onaantasbaar is (al is het probleem hier veel kleiner).

Daar wil een bedrijf als Vectra op inspelen. "We schrijven software om *security operations* te versterken, specifiek voor beveiligingsproblemen die ze nooit eerder zagen, en telkens onderzoeken we of het om een nieuwe aanvalsmethode gaat. Dat vraagt in de ontwikkelingsfase veel 'manuele' input, maar we automatiseren ons systeem met machinelearning-algoritmes, " legt Mike Banic, vicepresident voor marketing van Vectra, ons uit.

Vectra is op zich geen firewall of antivirus, maar wil uw it-afdeling wel wijzen op dreigingen en geeft aan waar u prioriteit aan moet geven. "We kunnen een aanval niet tegenhouden, maar we weten ze wel te vinden eens ze binnen zijn. Zo voorkom je dat hackers maanden ongemerkt je netwerk infiltreren en met (veel) data aan de haal gaan." Zo kunnen op duizend interacties gemakkelijk 850 securitygerelateerd lijken, maar lang niet allemaal zijn ze effectief een inbreuk of een groot gevaar. "Wij proberen dat te filteren tot zo'n 65 effectieve aanvalsgedragingen en van daaruit lijsten we dan een kleine dertig toestellen op die zeer waarschijnlijk zijn aangevallen. We geven ook een score op basis van dreigingsniveau en de waarschijnlijkheid dat er iets zal gebeuren, gebaseerd op eerdere observaties. Op die manier bespaar je je security operations team een pak werk."

Vectra gebruikt naar eigen zeggen een paar dozijn machinelearningtechnieken. "We komen elke maand met verbeterde algoritmes op basis van wat we in de wereld zien. 65 procent van onze klanten staat toe dat we hun data gebruiken om onze systemen slimmer te maken en hoe meer data sets, hoe rijker onze kennis en hoe preciezer we worden." Het gaat hier voor alle duidelijkheid om geanonimiseerde metadata. "Ik zie niet wat er in je mailbox zit, maar ik zie wel hoe het verkeer vanuit je toestel zich gedraagt en of dat aanvalsgedrag is of niet", verduidelijkt Chris Morales, hoofd security analytics bij Vectra. "We kunnen zelfs op een geëncrypteerd netwerk nog steeds aanvallen vinden."

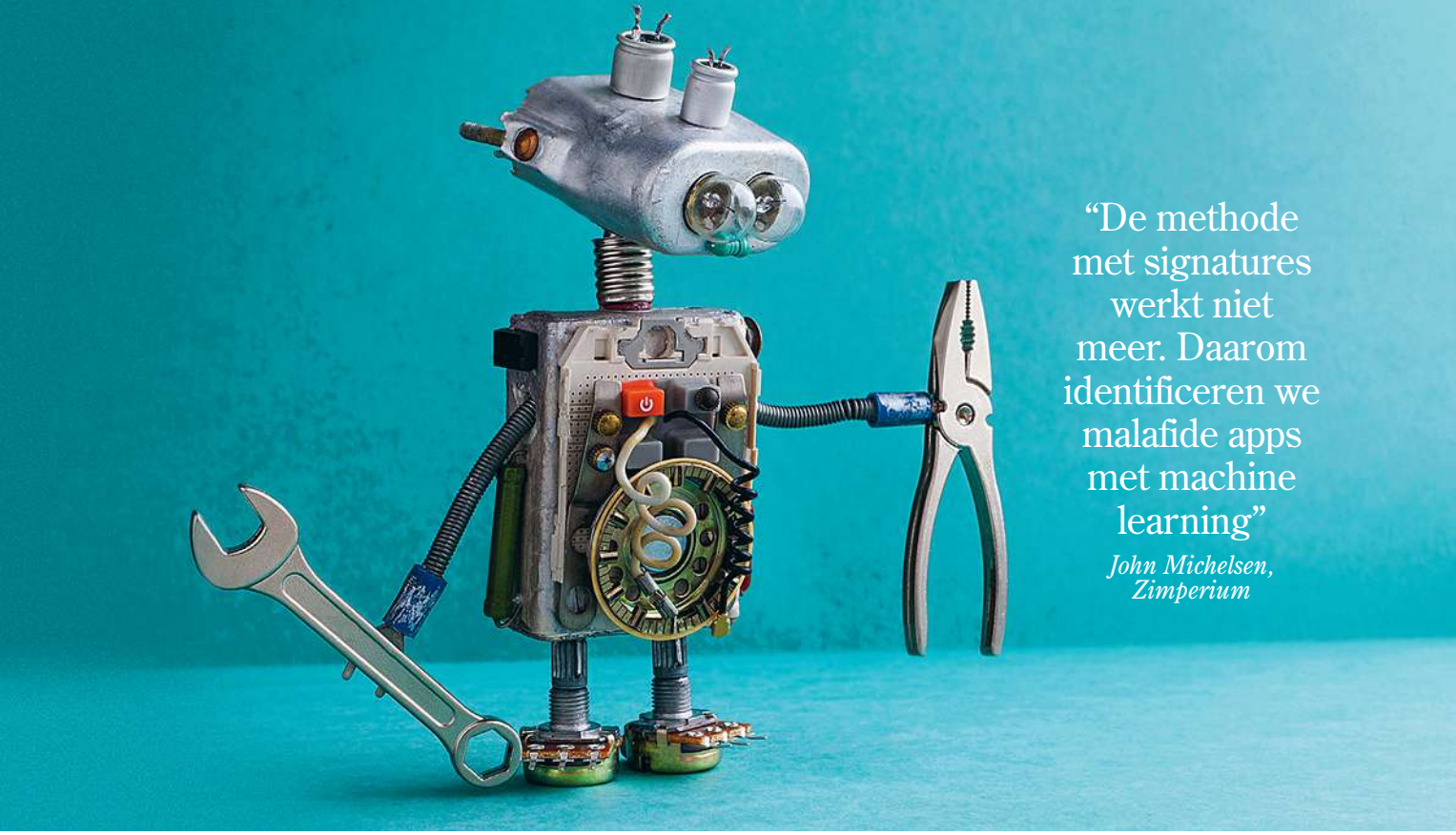
Vectra wordt onder meer ingezet in de financiële sector en het hoger onderwijs. "Daar zien we vaak botnets via toestellen van studenten binnenkomen. Maar de meeste onderwijsinstellingen weten intussen dat ze hen op een ander netwerk moeten zetten dan hun kritieke netwerkinfrastructuur," aldus Morales.

ORACLE

Wat het bedrijf doet, is niet uniek. We spreken Morales en Banic enkele dagen voor Oracle Openworld, waar cto Larry Ellison dezelfde kaart trekt in zijn keynote. "Het gaat om weten wanneer je wordt aangevallen. Als iemand rondneust in je computersysteem of een identiteit misbruikt dan moet je al op de hoogte zijn, voor ze verder infiltreren en met data gaan lopen."

"We moeten onze cyberbeveiliging automatiseren," zegt Ellison nog. "Computers kunnen vandaag beter gezichten herkennen dan mensen, diezelfde technologie gebruiken we nu om onze cybersecurity gedeeltelijk te automatiseren en op termijn zelfs volledig te automatiseren."

Als voorbeeld geeft de cto van Oracle patroonherkenning aan. "We produceren miljoenen *logs* per dag, voor hardware, software, storage, het netwerk, het OS of de virtuele machines. We houden het bij als iemand een *table* aanmaakt of *query* uitvoert. Door al die data samen te bren-



> "De methode met signatures werkt niet meer. Daarom identificeren we malafide apps met machine learning"
>
> *John Michelsen, Zimperium*

gen, kunnen we het systeem trainen om normale en abnormale patronen te onderscheiden."

Ook Hank Skorny, senior vicepresident voor IoT bij Neustar, dat identiteitsbeheer doet, wijst op de nood om niet enkel de toegang tot, maar ook de activiteit op uw netwerk of systeem automatisch te monitoren: "Je moet vanuit een identificeringsstandpunt altijd twijfelen aan de betrouwbaarheid. Je moet niet alleen controleren wie toegang krijgt op een systeem, maar ook monitoren wat sommige actoren op je systeem doen. Dat kan soms in enkele seconden gebeuren en dan kunnen ai en machine learning zeker helpen om bedreigingen op te merken voordat mensen ze kunnen vinden."

MALWARE NIET LANGER HET BREEKIJZER

Dat aanvallen automatisch worden herkend, maakt ook dat bepaalde trends makkelijker op te merken zijn. "Een jaar geleden zou ik je vertellen dat we vaak malware zien om de eerste inbreuk te forceren en zo zou een aanvaller lateraal bewegen, meer machines infecteren en zijn rechten op dat netwerk vergroten om verder te geraken in het systeem", zegt Chris Morales van Vectra. "Nu zien we aanvallen zonder malware. Ze breken in met iemands gebruikersnaam of wachtwoord, of via een softwareapplicatie waar ze rechtstreeks of onrechtstreeks toegang tot kunnen bemachtigen."

MOBILE

Voor de bescherming van mobiele toestellen kan machine learning eveneens ingezet worden. Dat is onder meer het domein van Zimperium, dat zich richt op iOS, Android en het Universal Windows Platform. "We leveren onze detectietechnologie als een app, maar ook als een SDK waarmee bedrijven het zelf kunnen doen", zegt John Michelsen, chief product officer bij Zimperium.

"Zo kunnen we zowel gekende als ongekende aanvallen detecteren. Toen de Dirty Cow exploit opdook, moesten veel securitybedrijven nagaan of hun klanten beschermd waren. Wij hadden de onze al ingedekt. Ook al kenden we het probleem niet, het werd automatisch ontdekt. Op die manier doen we ook veel meldingen, we hebben er ooit een zevental aan Apple gemeld waardoor ze kort nadien een nieuwe release van iOS moesten uitrollen", aldus Michelsen. "De methode met *signatures* (de unieke 'handtekening' die malware nalaat, nvdr) werkt niet meer. Daarom identificeren we malafide apps met machine learning. We hebben onze software de laatste 18 maanden getraind om te herkennen of een app foute dingen doet of niet. Ongeacht wat het precies is, er is altijd een beweging en die detecteren we."

De kracht van het algoritme loopt overigens niet enkel via de cloud. De machinelearningmechanismen zitten in de app ingebakken. Volgens de ontwikkelaars voegde dat maar 9 megabyte extra aan de app toe. Elke app wordt bij installatie of bij een update gescand, wat een dertigtal seconden kan duren. Maar wat dan met malware die pas achteraf actief wordt? "Vaak komt het pas in de dagen nadien via wifi of zelfs Bluetooth binnen. Of via mediabestanden. Maar zodra er iets verdachts op het toestel gebeurt, is de kans groot dat ons algoritme het opmerkt", besluit Michelsen.

De afgelopen jaren zagen we machine learning en kunstmatige intelligentie opduiken in het constateren van ziektebeelden of het herkennen van fraude. Maar ook securitybedrijven passen de technologie vandaag toe en zelfs een gigant als Oracle trekt de kaart voor zijn eigen producten. Het kat-en-muisspel tussen hackers en beveiligers stapt zo in een nieuw hoofdstuk. De ene moet zo snel en concreet mogelijke een onbekende dreiging herkennen, de andere moet voortaan zo voorzichtig mogelijk handelen om het geautomatiseerde alarm niet te laten afgaan.